

TCP Increased Security (tcpinc)

Chairs: Marcelo Bagnulo <marcelo@it.uc3m.es>
Tero Kivinen <kivinen@iki.fi>

Area Director: Martin Stiemerling <mls.ietf@gmail.com>
Tech Advisor: Stephen Farrell <stephen.farrell@cs.tcd.ie>

Mailing List
Address: tcpinc@ietf.org
To Subscribe: <https://www.ietf.org/mailman/listinfo/tcpinc/>
Archive: <http://www.ietf.org/mail-archive/web/tcpinc/>

Note Well

Any submission to the IETF intended by the Contributor for publication as all or part of an IETF Internet-Draft or RFC and any statement made within the context of an IETF activity is considered an "IETF Contribution". Such statements include oral statements in IETF sessions, as well as written and electronic communications made at any time or place, which are addressed to:

- The IETF plenary session
- The IESG, or any member thereof on behalf of the IESG
- Any IETF mailing list, including the IETF list itself, any working group or design team list, or any other list functioning under IETF auspices
- Any IETF working group or portion thereof
- Any Birds of a Feather (BOF) session
- The IAB or any member thereof on behalf of the IAB
- The RFC Editor or the Internet-Drafts function

All IETF Contributions are subject to the rules of RFC 5378 and RFC 3979 (updated by RFC 4879).

Statements made outside of an IETF session, mailing list or other function, that are clearly not intended to be input to an IETF activity, group or function, are not IETF Contributions in the context of this notice. Please consult RFC 5378 and RFC 3979 for details.

A participant in any IETF activity is deemed to accept all IETF rules of process, as documented in Best Current Practices RFCs and IESG Statements.

A participant in any IETF activity acknowledges that written, audio and video records of meetings may be made and may be available to the public.

Agenda

- Administration, 5 min
 - Agenda Bashing
 - Minutes, Jabber scribe
- Intro – Chairs and Technical Advisor, 10 min
- Presentation of proposals
 - Tcpcrypt – Andrea, 20 min
 - TLS - ekr, 20 min
 - DTLS – Martin, 20 min
 - TCP-AO – Joe, 20 min
- Way forward – all 25 min

Intro

- TCP extensions to provide unauthenticated encryption and integrity protection of TCP stream
 - Without modifications to upper layers
 - Forward security with per-connection granularity
 - NAT/firewall traversal
 - Key rollover without significant impact
 - Low overhead
 - No manual configuration
- (From charter)

Wish list from chairs

- We will only standardize one solution
- We will pick a solution sooner rather than later
- We will pick starting point, final solution can be significantly changed during the process
- Would like to get implementations sooner than later

Presentations

- Tcpcrypt – Andrea, 20 min
 - draft-bittau-tcpinc
- TLS - ekr, 20 min
 - draft-touch-tcp-ao-encrypt
- DTLS – Martin, 20 min
 - draft-rescorla-tcpinc-tls-option
- TCP-AO – Joe, 20 min
 - draft-thomson-tcpinc-dtls

Way Forward

- Discussion
- Open questions for WG:
 - Whether to protect TCP header
 - API